



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 4450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/724.034

11/26/2003

Markus Jakobsson

081004.179 US2

7279

21323 7590 02/22/2007
TESTA, HURWITZ & THIBEAULT, LLP
HIGH STREET TOWER
125 HIGH STREET
BOSTON, MA 02110

EXAMINER

LEMMA, SAMSON B

ART UNIT

PAPER NUMBER

2132

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
--	-----------	---------------

3 MONTHS

02/22/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/724,034

Applicant(s)

JAKOBSSON ET AL.

Examiner

Samson B. Lemma

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 November 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 2-85 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 2-85 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 09/02/2004.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This is in reply to application filed on November 26, 2003. Claim 1 is canceled.

Thus the remaining claims 2-85 have been examined.

Priority

2. This application claims priority of a provisional application, application No. 60/429754 filed on **November 27, 2002**. Therefore, the effective filing data for the subject matter defined in the pending claims of this application is **11/27/2002**.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. **Claims 2-72** are rejected under 35 U.S.C. 102(a) as being anticipated by **Secure computing corporation: "Authentication Reference Guide"** (Hereinafter referred as **Secure Computing**) (Publication date: April 9, 2002) (Pages 1-18, XP002283680, Submitted with the IDS)

5. **As per independent claims 2, 26, 43 and 57 Secure Computing discloses a method for generating an identity authentication code** [See pages 11-12 and 14-16,

Art Unit: 2132

"dynamic password"] associated with an authentication device, [See pages 11-12 and 14-16, "Authenticator/token"] comprising the steps of:

- **Providing event state data that specifies a condition of the authentication device; [See pages 11-12 and 14-16, "challenge/response"];**
and
- **Generating an identity authentication code [See pages 11-12 and 14-16, "dynamic password"] that depends at least in part on (i) a dynamic value, [See pages 11-12 and 14-16, "challenge"] (ii) the event state, [See pages 11-12 and 14-16, "response"] and (iii) a secret associated with the device. [See pages 11-12 and 14-16, "pin"]**

6. **As per dependent claims 3, 27, 44 and 58 Secure computing discloses a method as applied to claims above. Furthermore secure computing discloses the method wherein, the identity authentication code further depends on a dynamic value. [See pages 11-12 and 14-16, "challenge"]**

7. **As per dependent claims 4, 28, 45 and 59 Secure computing discloses a method as applied to claims above. Furthermore Secure computing discloses the method, wherein the dynamic value includes one or more of a time value, a challenge, and a counter. [See pages 11-12 and 14-16, "challenge" and see on page 12, "time-synchronous authentication and on page 11, see "The cryptoalgorithm incorporated in the token uses a counter that stays "in sync" with the server based on the number of passwords generated]**

8. **As per dependent claim 6. Secure computing discloses a method as applied to claims above. Furthermore secure computing discloses the method, further including changing the event state data when the condition of the authentication device changes [See pages 11-12 and 14-16, "response/challenge"]**

Art Unit: 2132

9. **As per dependent claim 7 Secure computing discloses a method as applied to claims above. Furthermore Secure computing discloses the method, wherein the condition of the device is covertly encoded in the identity authentication code.** [See pages 11-12 and 14-16], (Generating an identity authentication code or "dynamic password" that depends at least in part on (i) a dynamic value/condition of the device or "challenge" (ii) the event state or, "response" and (iii) a secret associated with the device or "pin" *meets the recitation of the limitation*)
10. **As per dependent claim 8 Secure computing discloses a method as applied to claims above. Furthermore Secure computing discloses the method, wherein the event state data**[See pages 11-12 and 14-16, "challenge"] **is derived from an associated event secret.** [See pages 11-12 and 14-16, "pin"] *(the challenge is prompted to the user after the pin is entered by the user meets the limitation of the challenge is derived from the an associated pin/event secret)*
11. **As per dependent claims 9-10 and 30-34 Secure computing discloses a method as applied to claims above. Furthermore Secure computing discloses the method, further including periodically changing the event secret.** [See pages 11-12 and 14-16, "pin"] *("this is an inherent features of authentication device which uses a pin", in any authentication system pins are periodically changing for security purposes)*
12. **As per dependent claims 12-13 Secure computing discloses a method as applied to claims above. Furthermore Secure computing discloses the method, wherein the event state data includes one or more event state bits, a subset of bits** [See pages 11-12 and 14-16, "challenge"] **being employed in generating identity authentication codes** [See pages 11-12 and 14-16, "dynamic password"] **for different time intervals** [Pages 12-13] *(Time-synchronous authenticators also generate unique, dynamic passwords at fixed intervals, usually one per minute.)*

Art Unit: 2132

13. **As per dependent claims 14-16 Secure computing** discloses a method as applied to claims above. Furthermore secure computing discloses the method, wherein the condition of the authentication device includes information about whether a battery supplying power to the authentication device has fallen below an expected power level. *[See page 15] (See for instance just one type of authentication device driven by a batter on page 15, and an indication that battery of these devices are fallen below an expected power level is an inherent feature in any small handheld battery driven devices.)*
14. **As per dependent claims 17, 35-37, 49 and 65, Secure computing** discloses a method as applied to claims above. Furthermore Secure computing discloses the method, wherein the identity authentication code *[See pages 11-12 and 14-16, "dynamic password"]* further depends on one or more of a PIN, a password, *[See pages 11-12 and 14-16, "pin"]* data derived from a biometric observation, *[See page 17]* user data, verifier data and a generation value *[See pages 11-12 and 14-16, "challenge/response"]*
15. **As per dependent claims 18-19 and 29, 42, 50, 56, 66 and 72 Secure computing** discloses a method as applied to claims above. Furthermore Secure computing discloses the method, further including, before generating the authentication code *[See pages 11-12 and 14-16, "dynamic password"]* receiving user input data *[See pages 11-12 and 14-16, response or pin]*, wherein the user input data is at least one of a PIN, a password, *[See pages 11-12 and 14-16, "pin"]* and biometric data *[See page 17]*
16. **As per dependent claims 20-24, 38-41, 51-55, 67-71 Secure computing** discloses a method as applied to claims above. Furthermore Secure computing

Art Unit: 2132

discloses the method, further including, transmitting the identity authentication code to verifier. [*See pages 14-17, "authentication"*]

17. **As per dependent claim 25 Secure computing discloses a method as applied to claims above. Furthermore Secure computing discloses the method, further including the step of displaying the identify authentication code on the device.**

[*See page 15*]

18. **As per dependent claims 46-48 and 60-64 Secure computing discloses a method as applied to claims above. Furthermore Secure computing discloses the method, wherein the information about the user includes where the user is located. [See page 1, "*behavioral measurement of the user, or determine that the user is located at a place..*"]**

19. **Claims 73-85 are rejected under 35 U.S.C. 102(b) as being anticipated by Smithies et al (Hereinafter referred as **Smithies**) (U.S. Patent No. 6,091,835), Patent Date: 07/18/2000)**

20. **As per independent claims 73, 83-85 and dependent claims 74-77 and 80-82 Smithies discloses a method for verifying the correctness of an identity authentication code, comprising:**

- **Receiving authentication information including the identity authentication code generated by an authentication device that depends on (i) a secret associated with the device, and (ii) event state data that specifies a condition of the authentication device;**[See claims 1 and 58] (*Claim 1 recites the following which meets the limitation of the above recitation, "a computer system for creating a secure, tamper-resistant electronic transcript which memorializes the events of*

Art Unit: 2132

a user's affirmation, through the entry of a signature token, of an electronic transaction having terms, the system comprising: a. a transaction application module enabling an affirming party to create an electronic transaction; b. a transcript generator module; and c. a signature token verification module accepting the signature token from the affirming party." Furthermore claim 58 discloses the following which also meets the above recitation, *"a computer based system for recording a series of acts constituting the signing of an electronic document and assuring an affirming party's intent, comprising: presentation means presenting an electronic document to be signed to the affirming party, the presentation means allowing the affirming party to electronically examine the document by accepting an at least one document review affirming party input command and displaying an at least one portion of the document in accordance with the at least one document review affirming party input command, the presentation means displaying a declaration of intention indicating the intention of the affirming party towards the document; verification means verifying the identity of the affirming party by requesting identity information from the affirming party and accepting identity information from the affirming party; checksumming means creating a document checksum of the document; ceremony generating means generating ceremony information from: the presentation of the document to the affirming party; the at least one document review affirming party input command and the at least one portion of the document displayed)*

- o **Verifying the correctness of the identity authentication code, and determining the condition of the authentication device in response to the received identity authentication code.** [See claims 1 and 58] *(Claim 1 recites the following which meets the limitation of the above recitation, "a signature token verification module accepting the signature token from the affirming party, verifying the signature token and transmitting a verification signal to the transcript generator module; wherein the transcript generator module accepts the terms, confirms the acceptance of the terms by presenting prompts, allows the affirming party to affirm the terms, gathers forensic*

Art Unit: 2132

data surrounding the affirming party's affirmation and stores information related to the prompts, the forensic data and the verified token as separate data entities in a tamper-resistant transcript object." Furthermore, claim 58 discloses the following which also meets the above recitation, "verification means verifying the identity of the affirming party by requesting identity information from the affirming party and accepting identity information from the affirming party; checksumming means creating a document checksum of the document; ceremony generating means generating ceremony information from: the presentation of the document to the affirming party; the at least one document review affirming party input command and the at least one portion of the document displayed; and the at least one identity input event relating to the identity information; and storing the identity information, document checksum and ceremony information in a transcript object.")

21. **As per dependent claim 78 Smithies discloses a method as applied to claims above. Furthermore Smithies discloses the method wherein the authentication information further includes user identifier. [See column 43 and claim 43]**

22. **As per dependent claim 79 Smithies discloses a method as applied to claims above. Furthermore Smithies discloses the method wherein the authentication information further includes at least one of a PIN, a password, and biometric data. [See column 43 and claim 43]**

Claim Rejections - 35 USC § 103

23. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject

Art Unit: 2132

matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

24. **Claims 5 and 11** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Secure computing corporation: "Authentication Reference Guide"** (Hereinafter referred as **Secure Computing**) (Publication date: April 9, 2002) (Pages 1-18, XP002283680, Submitted with the IDS) in view of **Smithies et al** (Hereinafter referred as **Smithies**) (U.S. Patent No. 6,091,835), Patent Date: 07/18/2000)

25. **As per dependent claim 5 Secure computing discloses a method for generating an identity authentication code [See pages 11-12 and 14-16, "dynamic password"] associated with an authentication device, [See pages 11-12 and 14-16, "Authenticator/token"] comprising the steps of:**

- o **Providing event state data that specifies a condition of the authentication device; [See pages 11-12 and 14-16, "challenge/response"];**
and
- o **Generating an identity authentication code [See pages 11-12 and 14-16, "dynamic password"] that depends at least in part on (i) a dynamic value, [See pages 11-12 and 14-16, "challenge"] (ii) the event state, [See pages 11-12 and 14-16, "response"] and (iii) a secret associated with the device. [See pages 11-12 and 14-16, "pin"].**

Furthermore, Secure computing on Page 15 discloses the following "If the token is stolen, the thief cannot retrieve valid passwords from the token without the PIN; what's more, as soon as the token is reported stolen, the administrator can immediately disable it. This type of token can be configured for synchronous or asynchronous authentication."

Art Unit: 2132

Secure Computing does not explicitly disclose

- wherein the condition of the authentication device includes information about whether the device has been subjected to tampering.

However, in the field of endeavor **Smithies discloses**, the condition of the authentication device includes information about whether the device has been subjected to tampering. [See column 14]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of having a response to the event state like tampering as per teachings Smithies in to the method of as taught by **Secure Computing** for the purpose strengthening the authentication process and the integrity of the system. [See column 14, Smithies]

26. **As per dependent claim 11 the combination of Secure computing and Smithies discloses a method as applied to claim above. Furthermore, Secure computing discloses the method further including changing the event secret when the condition of the authentication device changes.** [See pages 11-12 and 14-16, "pin"] (*"this is an inherent features of authentication device which uses a pin", in any authentication system pins are periodically changing for security purposes*)

Conclusion

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-Form 892).

- a. **U.S. Patent No. 5, 251,259** discloses a method for generating an identify authentication code using different event state features as it is described on figure 3 and claim 1) comprising the steps of:
- o storing events in an authentication device (See for instance "frequency of use")

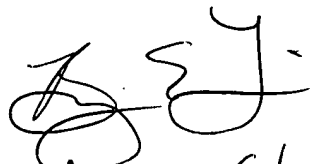
Art Unit: 2132

- o modifying the event state in response to an event ("See for instance "response") and
- o generating an identify authentication code that depends on at least in part on a dynamic value (day), the event state (number of usage) and a secret (Pin) associated with authentication device. Furthermore, the method discloses dynamic value associated with a time period or interval (See for instance, column 2)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA*S.L.*
02/20/2007
Benjamin E. Lanier
Examiner AU 2132